HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10004310-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): John Hall et al.

Confirmation No.: 3428

Application No.: 09/783,802

Examiner: Chai, Longbit

Filing Date: 02/12/2001

Group Art Unit: 2131

Title: System and Method for Authentication of a User of a Multi-Function Peripheral

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 06/07/2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$460.00
( )	three months	$1020.00
( )	four months	$1690.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of **$500.00**. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

( ) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit:_____

OR

(X) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571) 273-8300 on August 5, 2005

Number of pages: 18

Typed Name: Gloria L. Knox

Signature: Gloria L. Knox

Respectfully submitted,

John Hall et al.

By Michael J. D'Aurelio

Michael J. D'Aurelio

Attorney/Agent for Applicant(s)
Reg. No. **40,977**

Date: **August 5, 2005**

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10004310-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): John Hall et al.

Confirmation No.: 3428

Application No.: 09/783,802

Examiner: Chai, Longbit

Filing Date: 02/12/2001

Group Art Unit: 2131

Title: System and Method for Authentication of a User of a Multi-Function Peripheral

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

DUPLICATE

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 06/07/2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of **$500.00**. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

( ) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit:_____

OR

(X) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571) 273-8300 on August 5, 2005

Number of pages: 18

Typed Name: Gloria L. Knox

Signature: Gloria L. Knox

Respectfully submitted,

John Hall et al.

By Michael J. D'Aurelio

Michael J. D'Aurelio
Attorney/Agent for Applicant(s)
Reg. No. 40,977

Date: August 5, 2005

Telephone No.: (770) 933-9500

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In re the application of: John Hall et al.	Confirmation: 3428
Serial Number: 09/783,802	Art Unit: 2131
Filing Date: February 12, 2001	Examiner: Chai, Longbit
Title: SYSTEM AND METHOD FOR AUTHENTICATION OF A USER OF A MULTI-FUNCTION PERIPHERAL	Docket No.: 10004310-1
	Appeal Number: _____

APPEAL BRIEF UNDER 37 CFR §1.192

Mail Stop Appeal Brief—Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the decision of Examiner Longbit Chai, Group Art Unit 2131, of February 8, 2005, rejecting claims 1-18 in the present patent application and making the rejection final.

I. REAL PARTY IN INTEREST:

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249, Houston, Texas 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS AND INTERFERENCES:

There are no other appeals or interferences known to appellant that will directly affect or be directly affected by or have a bearing on the Board's decision in the present pending appeal.

III. STATUS OF CLAIMS:

Claims 1-18 are currently pending in the present application. The Final Office Action mailed on February 8, 2005 rejected claims 1-18 under 35 U.S.C. §103(a) as being unpatentable over US Patent Application Publication 2002/0116620 A1 filed by Gimbert. Applicants appeal the decision of the Examiner in rejecting claims 1-18. For the reasons set forth herein, Applicants respectfully submit that the rejection of the pending claims 1-18 should be overturned by the Board of Patent Appeals.

IV. STATUS OF AMENDMENTS:

With respect to claims 1-18, no amendments to the claims were submitted in this case. Thus, there are no amendments that have not been entered with respect to claims 1-18 before the issuance of the Final Rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER:

The invention as set forth in the present claims is described in the specification, for example at page 6, lines 6-15; page 7, line 3 through page 8, line 33, page 9, line 7-24, and page 9, line 4 through page 12, line 14. However, various related aspects of the present invention as described in the claims may be described elsewhere in the specification as well.

According to the various embodiments of the present invention, in one example the use of the multi-function peripheral (MFP) 105 and the server 110 in the context of a specific scanning and sending task is provided. To begin, a user wishes to use the MFP 105 to scan a hardcopy document into a digital document and then send the digital document to a number of recipients over a network 125. The user enters a number of destination email addresses 141 of the intended recipients of the

digital document into the MFP 105 and then initiates a send function where the digital document is distributed via email to the intended recipients. In doing so, the actual digital document is not transmitted to each recipient, but is posted on the web server 203 to be accessed by those recipients for which a destination email address 141 was entered.

Specifically, the digital sender 195 of the MFP 105 sends the digital document and the list of destination email addresses 141 to the digital sender service 201 of the server 110. The digital sender service 201 converts the digital document received from the digital sender 195 into a format that may be accessed via the web server 203. The digital sender service 201 then copies the digital document to the web server 203 where it may be accessed by the various devices coupled to the network 125, *etc.*

Next, the digital sender service 201 allows access to the digital document stored on the web server 203 to selected recipients by adding read file privileges in the access control list of the digital document. This is accomplished by associating the security identifier 143 for each appropriate recipient with the digital document. Specifically, the respective security identifiers 143 are listed in the access control list of the digital document. To accomplish this, the digital sender service 201 needs the security identifiers 143 associated with each of the destination email addresses 141 received from the digital sender 195.

This is achieved by mapping each of the destination email addresses 141 to a respective security identifier 143. Specifically, each of the destination email addresses 141 is sent to the directory server 120 along with a request for the security identifier 143 associated therewith. The requests are formatted according to a lightweight directory access protocol (LDAP) or other suitable protocol employed to access the information contained in the directory server 120. For each request, the directory server 120 then looks up the specific security identifier 143 and sends it back in a reply to the digital sender service 201.

Thereafter, the digital sender service 201 generates and transmits an email message to each of the intended recipients of the digital document based on the destination email addresses 141. A uniform resource locator (URL) that provides the location of the digital document on the web server 203 is associated with each of the email messages. Each of the email messages informs the recipient that they may access the digital document at the URL.

Each of the recipients may access the digital document based on the URL using, for example, a browser on a client device such as, for example, a computer system or other device that is coupled to the network 125. When accessing the digital document stored on the web server 203, the client device is authenticated using various techniques that are generally known by those with ordinary skill in the art. In requesting access to the digital document, the client device transmits the associated user identifier that may comprise, for example, the username and domain name to the web server 203 to perform the authentication. During the authentication process, the web server 203 may send, for example, the user identifier and/or other credentials to the domain controller 115 (FIG. 1) with a request for the associated security identifier 143 according to the lightweight directory access protocol. The directory server 120 responds with the associated security identifier 143. The web server then compares the security identifier 143 with those stored in the access control list of the digital document to determine who has access thereto. If the client has access, then the digital document is transmitted to the client accordingly.

Also, claim 11 is the only independent claim involved in the appeal that includes means-plus-function elements. Specifically claim 11 recites "means for mapping from a number of destination addresses to a respective number of security identifiers" various embodiments of which are described, for example, at page 4, lines 8-19; page 7, lines 14—page 8, line 25; page 10, lines 4-27; and page 11, line 3—page 12, line 14, (*i.e.* elements 120, 141, 143, 110, and 201); "means for adding a number of access privileges to the digital document via a network using the security identifiers", various embodiments of which are described, for example, at page 7, line 14—page 8, line 3; page 10, lines 16-27; and page 11, line 3—page 12, line 14 (*i.e.* elements 110, 201, 203); and "means for posting the digital document on a server accessible via the network," various embodiments of which are described, for example, at page 5, lines 3-11; page 7, line 3—page 8, line 25; page 10, line 16-27, page 11, and line 3—page 12, line 14 (*i.e.* elements 201, 203, 110, 125).

In addition, claim 13 is the only dependent claim involved in the appeal argued separately that includes a means-plus-function element. Specifically claim 13 recites "means for transmitting each of the destination addresses to the directory server along with a request for the security identifier associated therewith", various embodiments of which are described, for example, at page 7, line 29—page 8, lines 4-15; and page 11, line 3—page 12, line 14 (*i.e.* elements 201, 110).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:

Claims 1-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over US Patent Application Publication 2002/0116620 A1 filed by Gimbert.

VII. ARGUMENT:

Applicants believe that the simplest manner in which to examine the claims and rejections pertinent thereto is accomplished by looking at the key elements that the claims of the present application recite and that the cited prior art clearly lacks. Accordingly, the Applicants herein discuss the traversal of the rejections in light of the exemplary claims 1 and 3, respectively.

A. REJECTION OF CLAIMS 1-18:

Claims 1-18 have been rejected under 35 U.S.C. §103(a) as being unpatentable over US Patent Application Publication 2002/0116620 A1 filed by Gimbert. For the purposes of the following argument, Applicants present arguments traversing the rejection of claims 1-2, 4-7, 9-12, 14-16, and 18 with reference to representative claim 1. Also, Applicants separately present arguments traversing the rejection of claims 3, 8, 13, and 17 with reference to representative claim 3.

1. Gimbert falls to Suggest All of the Claimed Limitations of Claims 1-2, 4-7, 9-12, 14-16, and 18:

It is well settled law that a prima facie case of obviousness is established only when the prior art teaches or suggests all of the elements of the claims. MPEP §2143.03, In re Rijckaert, 9 F.3d 1531, 28 U.S.P.Q2d 1955, 1956 (Fed. Cir. 1993). Applicant asserts that Gimbert fails to show or suggest each of the elements of claims 1-2, 4-7, 9-12, 14-16, and 18 as originally filed. To begin, claim 1 as originally filed provides as follows:

> 1. A method in for transferring a digital document, comprising the steps of:
> mapping from a number of destination addresses to a respective number of security identifiers via a directory server;

adding a number of access privileges to the digital document in a computer system via a network using the security identifiers; and

posting the digital document on a server accessible via the network.

With respect to claim 1, the Office Actions states:

"Gimbert teaches a method in for transferring a digital document, comprising the steps of:
a. mapping from a number of destination addresses to a respective number of security identifiers via a director server (Gimbert: see for example, paragraph [0016] line 10-20): Gimbert discloses (a) the identity of the user must exist in the system's directory before the security system allows the access and the security system on the web server correlates the identity of the user entered with a list in the system's directory, and (b) an electronic mail notification to users associated with the document will be triggered in various events such as modification of documents (Gimbert: see for example, Paragraph [0016]). Therefore, the security identifiers must map to destination addresses in order to trigger the electronic mail notification to users.)" (Final Office Action of 2/8/2005, page 3).

Applicant respectfully disagrees. Gimbert fails to show or suggest mapping a number of destination addresses to a respective number of security identifiers in a directory server of a network. Also, the specific statement in the Office Action that "the security identifiers must map to destination addresses in order to trigger the electronic mail notification to users" is erroneous and misinterprets the fair teachings of Gimbert.

Gimbert teaches a system that allows users to access, create, and modify documents used in regulatory proceedings for a government entity. In order for any user to access the system, they must provide a username and a password. Before a user may actually log into the system as such, their name and password have to be entered into the system by an administrator to provide access. Once a user logs onto the system, they may create a document that is then viewed by a number of individuals as described in paragraph [0022] of Gimbert which states:

In one sequence of steps according to FIG. 2, an employee of the entity enters the system at step 38 and after viewing their personal task list at step 40 proceeds to input a document at step 44 as may be required by law, such as a document for certification of a product or service, in fulfillment of an action item on their task list shown at step 40. To input a document, the employee of the entity goes to the systems' page within the server that is used to create a document 44.

> Then entity employee uses the fields in the web form to create the document and/or may attach computer files that are the document or related to the document itself. After the document is created or attached, the entity employee selects the appropriate supervisor that the completed document will be sent to for review and revision at step 46 before the document is submitted to the entity-agency liaison at step 48. The selected supervisor receives the request to review the newly created document in one of two ways, by automatically adding revision of document to the supervisor's personal task list on the web server and/or by an automatic electronic mail message. Both the personal task list and the email massage contain hypertext link to the document. The supervisor then enters the system via steps 38 and 40, then proceeds to the review step 46. The document is then sent to the entity-agency liaison at step 48. The entity-agency liaison also enters the system via steps 38 and 40, then proceeds to the review step 48. After the entity-agency liaison receives the document, the entity-agency liaison may submit the document to the agency which generates an automatic email notification to the agency at step 50. **Throughout the process, any time a document, question, response, etc., is sent from one individual or role to another, whether within the entity, within the agency, or across the entity-agency border, the recipient's task list is updated and an automatic email notification sent.** (Emphasis Added)

Thus, there are no "security identifiers that are used to map to destination addresses in order to trigger the electronic mail notification to users" as stated in the Office Action. Rather, individual users specify to whom a document is to be sent and the automated email message is sent out. The potential recipients are necessarily stored in the system to that a user can specify that such recipient is to receive notification.

This is in contrast to the invention as set forth in claim 1. Specifically, a number of destination addresses are mapped to a corresponding number of security identifiers. Access privileges are associated with a document using the security identifiers and the document is posted for access. Gimbert teaches that users must log into a system to gain access to the system in general. Gimbert does not teach the use of security identifiers to restrict access to specific documents. Rather, Gimbert teaches that individuals are provided access as they are identified by users who act upon a document as described above. In this respect, Gimbert teaches away from mapping destination addresses to security identifiers.

Nonetheless, in response to Applicant's arguments, the Final Office Action further states:

> "Applicant remarks "Gimbert fails to show or suggest mapping from a number of destination addresses to a respective number of security identifiers via a directory server". Examiner notes Gimbert discloses (a) the identity of the user must exist in the system's directory before the security system allows the access and the security system on the web server correlates the identity of the user entered with a list in the system's directory, and (b) the web server utilize an automatic email program to notify designated users concerning the approval of a document, rejection of a document, modification of a document that could trigger an email notification to users associated with the document (Gimbert: see for example, Paragraph [0016] Line 1-11). Therefore, Examiner notes the email address must include the destination addresses of all of the users associated with (i.e. concerning) the particular document posted in the web server (e.g. upon the approval or rejection or modification of a particular document (e.g. "DoD Aircraft Design Document"), all of the engineers and managers associated with this particular document in a particular project team will receive the email notification (interpreted as the destination address with respect to the source address of digital document sender)." (Final Office Action of 2/8/2005, page 2).

The Final Office Action overstates the teachings of Gimbert. While the identity of a user does exist in the system's directory, the identity of a user is tracked with usernames and passwords that relate to email addresses. Also, even though an automatic email program is employed to notify users of the need for action with respect to a document, individual users specify to whom the notification is to be made and there is no security identifier accessed to determine access privileges to a document as claimed. Rather, security is provided by requiring all users to log in with a username and password when they access the system and then act upon the document for which the email notification was delivered.

In addition, the specific statement that the "Examiner notes the email address must include the destination addresses of all of the users associated with (i.e. concerning) the particular document posted in the web server (e.g. upon the approval or rejection or modification of a particular document" is confusing. How does an "email address" include "destination addresses"? As stated above and set forth in paragraph [0022], Gimbert teaches that users who create a document or review a document specify the next user or users to whom notice is to be sent.

Also, in support of the above contentions, the Final Office Action cites a specific example stating:

> "upon the approval or rejection or modification of a particular document (e.g. "DoD Aircraft Design Document"), all of the engineers and managers associated with this particular document in a particular project team will receive the email notification (interpreted as the destination address with respect to the source address of digital document sender)". (Final Office Action of 2/8/2005, page 2).

as proof that a number of users associated with a document receive email notification. To the extent that Gimbert teaches that users receive email notification, such individuals are specified by other users who act upon a document as described in paragraph [0022] set forth above. While notifying "all of the engineers and managers associated with a particular document in a particular project team" with an email notification appears impressive, a detailed review of Gimbert reveals that this example is not actually mentioned in the text. Specifically, there is no discussion of a team of individuals who are notified as such. Also, there is no mention of a "DOD Aircraft Design Document" as an example by Gimbert. About the closest Gimbert comes to this statement is at the end of paragraph [0012] which states:

> "One non-limiting example of an entity-agency pair would be an aircraft engine manufacturer seeking airworthiness certification from the FAA for a new engine model."

In any event, even if a team of individuals were mentioned as being associated with a document, such individuals would have to have been identified by a creator of the document or other person who acted upon the document at some point. There is no function in which a number of destination addresses are mapped to a respective number of security identifiers via a directory server, where the security identifiers are employed to provide access privileges to a document as set forth in claim 1. Rather, a simple login with a username and password is what limits user access to the system. The user then may view the document for which they received notification.

Given that the example above is not mentioned in the text of Gimbert, then it must necessarily be based on facts within the personal knowledge of the Examiner. Regulations specifically provide that when a rejection in an application is based on facts within the personal knowledge of an Examiner, it should be specific as possible. When called for by the Applicant, the Examiner must support the assertion with an affidavit which is subject to contradiction or explanation by the affidavits of

the Applicant or other persons. 37 CFR 1.104(d)(2). Applicant has expressly requested a formal affidavit from the Examiner testifying to the facts expounded upon in the Final Office Action to the extent that they are not fairly disclosed by Gimbert to no avail. (See Response to Final Office Action of February 8, 2005). No affidavit has been provided by the Examiner in this respect.

Accordingly, Applicant asserts that the rejection of claims 1 is improper. Also, Applicant asserts that the rejection of claims 6, 11, and 15 is improper for the same reasons provided about with respect to claim 1 to the extent that such reasons apply. Therefore, Applicant respectfully requests that the board overturn the rejection of claims 1, 6, 11, and 15. In addition, Applicants request that board overturn the rejection of claims 2, 4-5, 7, 9-10, 12, 14, 16, and 18 as depending from claims 1, 6, 11, or 15.

2. Gimbert fails to Suggest All of the Claimed Limitations of Claims 3, 8, 13, and 17:

As stated above, claims 3, 8, 13, and 17 have been rejected under 35 U.S.C. §103(a) as being unpatentable over *Gimbert*. Once again, it is well settled law that a prima facie case of obviousness is established only when the prior art teaches or suggests all of the elements of the claims. MPEP §2143.03, In re Rijckaert, 9 F.3d 1531, 28 U.S.P.Q2d 1955, 1956 (Fed. Cir. 1993). Applicant asserts that Gimbert falls to show or suggest each of the elements of claims 3, 8, 13, and 17 as originally filed. Claim 3 as originally filed provides as follows:

> 3. The method of claim 1, wherein the step of mapping from the number of destination addresses to the respective number of security identifiers via the directory server further comprises the step of transmitting each of the destination addresses to the directory server along with a request for the security identifier associated therewith.

With respect to claim 3, the Final Office Action states:

> "Gimbert as modified teaches the claimed invention as described above (see claim 1, 6, 11, and 15 respectively). Gimbert as modified further teaches mapping from the number of destination addresses to the respective number of security identifiers via the directory server further comprises the step of transmitting each of the destination addresses to the directory server along with the request for the security identifier associated therewith (Gimbert:

see for example, paragraph [0016] line 14-20)." (Final Office Action of 2/8/2005, page 5).

Once again Applicant respectfully disagrees. Specifically, if Gimbert does not teach mapping destination addresses to security identifiers as is described above, then Applicant asserts that Gimbert necessarily fails to show or suggest transmitting each of the destination addresses to the directory server along with a request for the security identifier associated therewith.

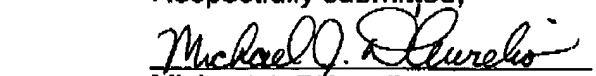
Thus, Applicant asserts that Gimbert fails to show or suggest the subject matter of claim 3. Also, Applicant asserts that Gimbert fails to show or suggest the subject matter of claims 8, 13, and 17 for the same reasons as stated above with respect to claim 3 to the extent such reasons apply. Accordingly, Applicant requests that the Board overturn the rejection of claims 3, 8, 13, and 17 for these additional reasons.

VIII. CONCLUSION:

In view of the foregoing, Applicants assert that claims 1-18 are in proper condition for allowance, and the Board is respectfully requested to overturn the Examiner's rejections of these claims.

Authorization is provided in the documents accompanying this Appeal Brief to charge Applicant's deposit account for the amount of $500.00 to cover the fee associated with filing this Appeal Brief. If any additional fees are required for this Appeal Brief to be considered, Applicant hereby authorizes the Board to charge any additional fee that may be required to deposit account 08-2025.

Respectfully submitted,



Michael J. D'Aurelio
Reg. No. 40,977

Thomas, Kayden, Horstemeyer & Risley, L.L.P.
100 Galleria Parkway, N.W.
Suite 1750
Atlanta, Georgia 30339-5948
Phone: (770) 933-9500
Fax: (770) 951-9300

IX. CLAIMS APPENDIX:

The claims as currently pending are as follows:

1. A method in for transferring a digital document, comprising the steps of:

mapping from a number of destination addresses to a respective number of security identifiers via a directory server;

adding a number of access privileges to the digital document in a computer system via a network using the security identifiers; and

posting the digital document on a server accessible via the network.

2. The method of claim 1, further comprising the steps of:

generating a number of email messages in the computer system to be transmitted to the number of destination addresses, respectively;

associating a uniform resource locator of the digital document on the network with each of the email messages; and

transmitting the email messages to the respective destination addresses on the network.

3. The method of claim 1, wherein the step of mapping from the number of destination addresses to the respective number of security identifiers via the directory server further comprises the step of transmitting each of the destination addresses to the directory server along with a request for the security identifier associated therewith.

4. The method of claim 3, wherein the step of adding the number of access privileges to the digital document in a computer system via the network using the security identifiers further comprises the step of listing the security identifiers received from the directory server in an access control list associated with the digital document.

5. The method of claim 4, further comprises the step of authenticating a client device attempting to access the digital document via the network.

6. A system for transferring a digital document, comprising:

a processor circuit having a processor and a memory;

a digital sender service stored on the memory and executable by the processor, the digital sender service comprising:

logic to map from a number of destination addresses to a respective number of security identifiers;

logic to add a number of access privileges to the digital document via a network using the security identifiers; and

logic to post the digital document on a server accessible via the network.

7. The system of claim 6, wherein the digital sender service further comprises logic to generate and transmit a number of email messages to a corresponding number of destination addresses on the network, wherein each of the email messages includes a uniform resource locator of the digital document on the network.

8. The system of claim 6, wherein the logic to map from the number of destination addresses to the respective number of security identifiers further comprises logic to transmit each of the destination addresses to the directory server along with a request for the security identifier associated therewith.

9. The system of claim 8, wherein logic to add a number of access privileges to the digital document via a network using the security identifiers further comprises logic to list the security identifiers received from the directory server in an access control list associated with the digital document.

10. The system of claim 9, wherein the digital sender service further comprises logic to authenticate a client device attempting to access the digital document via the network.

11. A system for transferring a digital document, comprising:

means for mapping from a number of destination addresses to a respective number of security identifiers;

means for adding a number of access privileges to the digital document via a network using the security identifiers; and

means for posting the digital document on a server accessible via the network.

12. The system of claim 11, further comprising means for generating and transmitting a number of email messages to a corresponding number of destination addresses on the network, wherein each of the email messages includes a uniform resource locator of the digital document on the network.

13. The system of claim 11, wherein the means for mapping from the number of destination addresses to the respective number of security identifiers further comprises means for transmitting each of the destination addresses to the directory server along with a request for the security identifier associated therewith.

14. The system of claim 13, wherein the means for adding the number of access privileges to the digital document via the network using the security identifiers further comprises means for listing the security identifiers received from the directory server in an access control list associated with the digital document.

15. A computer program embodied on a computer readable medium for transferring a digital document, comprising:

logic to map from a number of destination addresses to a respective number of security identifiers;

logic to add a number of access privileges to the digital document via a network using the security identifiers; and

logic to post the digital document on a server accessible via the network.

16. The computer program embodied on a computer readable medium of claim 15, further comprising:

logic to generate a number of email messages to be transmitted to the number of destination addresses, respectively;

logic to associate a uniform resource locator of the digital document on the network with each of the email messages; and

logic to transmit the email messages to the respective destination addresses on the network.

17. The computer program embodied on a computer readable medium of claim 15, wherein the logic to map from the number of destination addresses to the respective number of security identifiers further comprises logic to transmit each of the destination addresses to the directory server along with a request for the security identifier associated therewith.

18. The computer program embodied on a computer readable medium of claim 17, wherein logic to add the number of access privileges to the digital document via the network using the security identifiers further comprises logic to list the security identifiers received from the directory server in an access control list associated with the digital document.

X. Evidence Appendix:

No evidence is offered herein.

XI. Related Proceedings:

There are no copies of decisions rendered by a court or the Board to be provided herewith.